Accellion Share Securely™

AN ACCELLION WHITE PAPER

10 Mobile Security Requirements for the BYOD Enterprise

Accellion, Inc.
1804 Embarcadero Road
Suite 200
Palo Alto, CA 94303

Tel +1 650 485-4300
Fax +1 650 485-4308
www.accellion.com
info@accellion.com

WP-10BYOD0312

Executive Summary

Enterprises need to ensure that mobile workers always have the information they need at their fingertips and can share it with business partners and customers, while also ensuring that confidential data remains secure and that data security regulations and policies are never violated.

To meet the mobility and security requirements of road warriors and other mobile users, enterprises should deploy a solution that enables mobility of their content as part of their overall Enterprise Mobility Management (EMM) strategy; one that complements the basic provisioning and security services made available through Mobile Device and Mobile Application Management platforms.

An effective content mobility solution supports Bring Your Own Device (BYOD) policies, enables authorized users to share files of any size securely, gives IT managers fine-grained access controls for files and devices, and helps enterprises ensure that their mobile communications comply with internal data security policies and industry regulations. By making file sharing safe and convenient, a content delivery and control solution like Accellion enables road warriors to be as productive as possible on any device anytime, anywhere.

Same Mileage, New Complexity

Road warriors and mobile workers —sales people, business development managers, field technicians, and other users who spend most of their time on the road—remain as important as ever. Even in the age of social networks and 3G connectivity, face-to-face meetings and on-site visits remain indispensable for many aspects of business.

While the need for road warriors remains unchanged, the technology that road warriors are relying on has recently changed dramatically. Instead of using company-issued laptops, road warriors are increasingly carrying their own smartphones and tablets. And they're using these devices to connect not just to the home office and to business applications like SAP and Oracle, but also to remote partners and business-class and consumer-class cloud services, including social networks.

This creates new challenges for IT managers, directors of field operations, mobile device management (MDM) administrators, and other IT personnel who are responsible for provisioning devices and services for road warriors. People in these roles must ensure that mobile workers have the connectivity and services they need for productivity, while also ensuring that mobile operations never violate IT security policies or industrial regulations.

Here are five ways that provisioning for road warriors has become more complex:

- **BYOD Device Explosion**
  Five years ago, road warriors carried laptops and cell phones. If they carried smartphones, they were typically BlackBerrys, and the IT department configured and carefully managed smartphone communications through the BlackBerry Enterprise Server. Today, more than 70% of organizations have adopted, or at least embraced, a Bring Your Own Device (BYOD) policy for mobile users,[1] and iPhones and Android devices have become more popular than BlackBerrys. In addition, road warriors are also carrying iPads and other tablet devices. Nearly a third of mobile workers use more than one mobile device on a typical work day. Instead of standardizing on a single, coherent technology platform for mobile users, IT departments find themselves scrambling to accommodate this ever-changing heterogeneous environment. Even managing all the devices used by a single user might involve supporting Windows (for a laptop), iOS (for an iPad), and Android (for a Droid smartphone).
- **More Locations**
  The number of public Wi-Fi hotspots in the United States nearly doubled in 2011.[2] Instead of connecting to networks only in trusted locations such as branch offices, mobile workers today are connecting to networks just about everywhere: in airports, hotels, conference centers, cafes, restaurants, and trains—as well as home offices. Inadequately secured mobile devices are more exposed than ever before to hackers who monitor traffic on open networks.
- **More Apps and Services**
  Five years ago, the mobile app market was nonexistent. Road warriors with laptops could browse the Web, but tablets weren't popular (they were basically lidless laptops), and smartphones supported corporate email and calendaring and little else. Today there are more than 500,000 apps in the Apple App Store and more than 200,000 apps in the Android Marketplace. In addition, a large

[1] http://www.good.com/resources/Good_Data_BYOD_2011.pdf
[2] http://www.jiwire.com/sites/default/files/JiWire_MobileAudienceInsightsReport_Q32011_0.pdf

number of cloud-based services have become popular for everything from contact management to booking travel to managing expenses.

- **More People**
  Five years ago, the reliance on email limited the number of people with whom a road warrior could communicate. Email security rules might restrict email recipients to fellow employees and trusted partners. Large files would be sent by FTP, limiting their circulation to those who could be trusted with FTP accounts. Today, the profusion of applications and social networks makes it easier than ever for road warriors to communicate with colleagues, prospects, customers, partners, and anyone else who might be participating in a forum or social network.
- **More Media Types**
  Smartphones with embedded cameras and the rising popularity of video have made multimedia files much more popular. Workers on-the-go still send and receive Word documents, Excel spreadsheets, and PowerPoint presentations, but they also now work with JPG photos, MP3 podcasts, video files and other multimedia.

Supporting mobile workers who carry more devices, use more apps and services, connect from more locations, communicate with more people, and work with more media types would keep IT departments busy enough. But there's yet another development that makes supporting these folks a matter of pressing importance: a lot more employees are adopting the mobile lifestyle.

Adopting the Mobile Life Style

Until recently, road warriors were the mobile exceptions to the enterprise workforce. Field technicians and sales people traveled, but your typical business person worked at a desk with a desktop computer and a land line.

In the past few years, though, a sizeable portion of the workforce has adopted the mobile habits of the road warrior. They now work from their BYOD smartphones and iPads and/or a provisioned device some of the time and access corporate IT services from locations as varied as home offices, cafes, and airports.

Consider these statistics:

- 3 out of 5 workers say they no longer need to be in the office to be productive.[3]
- IDC estimates that by 2015 there will be over 200 million mobile workers in the United States.[4]

By addressing the IT security and productivity needs of road warriors, enterprises can also address the needs of the growing number of co-workers who are almost as mobile or already as mobile as traditional road warriors.

[3] Cisco quoted by Gist.com.
[4] http://esj.com/articles/2012/01/23/Mobile-Workforce-Growth.aspx

Why Mobile Device Management Is Not Enough

To help IT departments provision, manage, and secure their mobile devices, about a third of enterprises have deployed Mobile Device Management (MDM) solutions.[5] MDM enables IT organizations to provide over-the-air (OTA) updates of applications, configuration settings, and data to mobile devices, including smartphones and tablets. IT managers can use MDM systems to control which mobile devices are granted access to internal resources. Should a mobile device be lost or stolen, IT managers can use MDM to wipe the device remotely the next time it connects to the Internet.

MDM solutions provide a useful framework of provisioning mobile devices and mobile apps and for enforcing fundamental device-security controls. But MDM solutions do not address all the file-sharing and collaboration needs of road warriors.

Road warriors will be most productive if they can send and receive files of any type and size to authorized users inside and outside the organization. Because they're on the road, rather than in a conference room back in the office, it's also helpful if they have as much context as possible about files. Examples of context include comments and threaded discussions about the files being worked on, as well as automatic notifications being sent when files change. Providing rich context also includes integrating with content management systems such as Microsoft SharePoint, where increasingly important business files are stored.

Almost all MDM solutions provide basic app and data provisioning, but they do not provide a full content mobility solution -- capabilities needed to securely extend the enterprise content to mobile users -- for securely integrating flexible corporate file access, sharing and collaboration practices and services provisioned in the office.

Risky Consumer-Class Services

To share files across devices, many mobile workers are turning to consumer-class file-sharing services such as Dropbox. Unfortunately, services like Dropbox lack the rigorous controls that enterprises need for protecting data and maintaining regulatory compliance. Once users entrust their files to these services, IT departments have no way to monitor or control how the files are distributed and who has access to them. Besides increasing the risk of a data breach, this lack of control often puts organizations out of compliance with data security regulations such as GLBA, HIPAA, NASD, and SOX. Recent data breaches, such as Dropbox accidentally removing password-protection for all files for all users for 4 hours, only highlight the dangers of entrusting confidential data to these services.

There's another reason for IT to provide a secure mobile file sharing solution rather than let users pick their own services. Letting different users pick different services for sharing and managing the same corporate data only increases the complexity of mobile security. BYOD is complex enough. Adopting an ad hoc mix of Dropbox and other free file-sharing services only increases that complexity, making data security exposures nearly impossible to manage. Call it BYOFSS (Bring Your Own File-Sharing System) over BYOD (Bring Your Own Device), or call it just chaotic and risky. Enterprises need a coherent, comprehensive solution for secure file sharing across mobile devices.

[5] http://www.informationweek.com/news/mobility/business/229402912?pr

Devices and Files Everywhere

End users, meanwhile, remain imprudently enthusiastic. Millions of them are signing up for free file synchronization services.[6] These services promise a hassle-free solution to many bothersome IT challenges. File synchronization is a 21st century solution to the plight of the 21st century mobile professional.

Users are juggling more devices than ever before. They have computers at work, computers at home, smartphones, and tablets. Through websites and web applications, they can access their personal data (email, social network feeds, blog posts) from any of these devices, and they'd like to be able to do the same with their professional data. The iPad that serves up video clips, weather reports, and family email on a Saturday, ends up accessing business applications and business email on Monday. File synchronization makes this possible.

So does the architectural shift that's taking place in enterprise and consumer IT. The age of "fat clients" and PC-only applications is gone. Web services and mobile apps are the new platforms for business. To bring work data to personal devices,

Mobile Security Threats

A recent survey found that enterprise IT teams were most concerned about the following types of mobile security threats:

- *Loss or theft of a device carrying sensitive information: 64%*
- *A malware-infected device connecting to an internal network: 59%*
- *A malware-infected app being downloaded to a mobile device: 37%*
- *Data leak from user uploading confidential data to a mobile device: 36%*

A rise in the popularity of mobile devices corresponds with a rise in data breaches. For example, a study by Manhattan Research found that when doctors' use of smartphones rose by 9%, data breaches rose 32%[7].

10 Requirements for a Secure Mobile File Sharing

IT managers responsible for deploying mobile services for road warriors should consider these requirements when selecting a mobile content security solution:

1. **Multi-Device Support**
   The optimal secure content mobility solution supports whatever mix of mobile devices mobile users are carrying. In organizations that have adopted BYOD policies, iOS and Android devices are replacing the BlackBerry, but all three platforms remain popular. A single user may have one of each. A secure mobile file-sharing service should support all three platforms, which today constitute over 95% of smartphones and tablets in use.

2. **File- and Workspace-based Security**
   The solution should enforce strict access controls for individual files and for shared workspaces. Mobile employees often work with sensitive data, such as sales contracts and business plans. Therefore, files should be encrypted at rest, in transmit over SSL, and even protected if left open on a device that is not being used. File owners and administrators should be able to set expiration dates for files, so sensitive data isn't left exposed on servers. A mobile file sharing solution should ensure that mobile access never jeopardizes data security or regulatory compliance.

3. **Support for Secure Cross-boundary Collaboration**
   While keeping data secure, the solution should enable road warriors to share information securely across corporate boundary with external users such as partners and customers. Secure communications should not be limited to users inside the same domain.

[6] "Dropbox Hits 25 Million Users, Saves 200 Million Files Per Day," Michael Arrington, *TechCrunch,* http://techcrunch.com/2011/04/17/dropbox-hits-25-millions-users-200-million-files-per-day/.

[7] *Sources:* http://www.informationweek.com/news/mobility/business/229402912, http://www.ama-assn.org/amednews/2011/12/19/bil21219.htm

4. **Context for Files**
   The solution should include secure workspaces that provide context for data, making it easy for mobile workers to track discussions, revisions and other activities on important files in order to provide context for files, making it easy for mobile workers to collaborate while on the go. For example, it's important for a mobile user to understand the context of why the team at headquarters has revised a contract that's about to be presented to a prospect. Collaborative workspaces capture these important details and make them available to all authorized users, including mobile users. This eliminates the need for perfunctory back-and-forth communications, such as long email threads about document revisions, and translates directly into productivity increases.

5. **App Stores that the IT Department Controls**
   The solution should have a mobile app that is supported (aka white-listed) by the enterprise app store (or MDM) solution vendor and included in the list of apps approved by the IT department. White listed apps are important as they minimize the risk of malicious apps compromising mobile devices. Enterprises should avoid risks such as the 58 malicious applications that were released in the Android marketplace in 2011, infecting 260,000 devices which later had to be wiped clean by Google. Restricting apps to those approved by IT eliminates this vector of attack and ensures enterprise management of software updates and data tracking.

6. **Secure Environments for Apps**
   Especially on consumer devices that also hold personal data, it's important for business data to be stored in a secure sandbox. In fact, for some enterprises, it is not enough to keep the business content secure. It's important that they keep personal data on the device private and outside of the corporate sandbox. The secure environment should include essential security features, such as anti-virus scanning. It should also enable administrators to restrict file access to view-only and to scrub devices that have been lost or stolen.

7. **Integration with Leading Content Management Systems**
   The solution should also extend mobile access to popular enterprise content management solutions such as SharePoint, Autonomy iManage, and File Net. It should offer plug-in components and permissions granted through admin controls that extend the data infrastructure that's already in place in enterprise data centers to authorized internal and external mobile users. These plug-in components make the mobile file sharing solution, and the mobile app, act as a window into an enterprise's entire content.

8. **Support for Large Files**
   The mobile file sharing solution should support large file sizes, since rich media files (videos, medical images) are becoming increasingly common across all industries. Users need to be able to share and discuss multi-gigabyte files, even if they're not downloading these files to every mobile device.

9. **Visibility, Management and Control for IT**
   Administrative dashboards and logging have to be an integral component of a fully deployed content mobility solution. Content delivery and control capabilities in a mobile file sharing solution give administrators the ability to assign roles, access rights, and implement security policies for departments, teams, and individuals. Complete visibility and control over mobile users' file access and sharing activities is needed to change content access security policies per projects and as changes occur in the enterprises.

10. **Industrial-strength Security for Regulatory Compliance**
    Security and audit controls that support compliance with industry regulations such as GLBA, HIPAA, and SOX. Ease-of-use and productivity can never come at the expense of

industry regulations and federal and state laws. Enterprises need to stay compliant while serving their mobile workforce.

To address these requirements, enterprises should deploy a secure Mobile File Sharing solution that brings the rules-based access, delivery, controls and logging associated with enterprise content management solutions to mobile devices.

Accellion secure enterprise content mobility solution gives mobile workers access to the critical business data they need, any time, any where, and on any device (authorized or not), including tablets and smartphones. Along with screening of devices and mobile apps, Accellion provides an essential layer of security and control of content for these highly productive mobile workers.

For information about Accellion Mobile File Sharing solution, please visit www.accellion.com.

About Accellion

The world's leading corporations and government enterprises rely on Accellion secure file sharing and collaboration solutions to secure their enterprise information and ensure compliance. Founded in 1999, Accellion, Inc. provides enterprise-class secure file sharing solutions that deliver the ease-of-use internal and external users need while giving the enterprise organization the protection it needs.

Accessible to employees and external users from the Web, iPad, iPhone, Android and Blackberry mobile devices, Accellion secure file sharing solutions offer the widest choice of deployment options spanning virtual and public, private, or hybrid cloud environments.

The company is headquartered in Palo Alto, California with offices in North America, Asia, and Europe. For more information please visit www.accellion.com or call (650)-485-4300. Follow Accellion Blog, Twitter, Facebook, and LinkedIn.

www.accellion.com **info@accellion.com**